United Nations A/63/139

General Assembly

Distr.: General
18 July 2008
English
Original: Arabic/Chinese/English/
French/Spanish

Sixty-third session
Item 87 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Contents

		Page
I.	Introduction	2
II.	Replies received from Governments	2
	China	2
	Cuba	3
	Jordan	5
	Lebanon	5
	Niger	6
	Qatar	8

* A/63/150.

08-42992 (E) 060808 080808

I. Introduction

1. In paragraph 3 of its resolution 62/17, the General Assembly invited all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level.

2. Pursuant to that request, on 15 February 2008, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

China

[Original: Chinese]
[15 May 2008]

1. The rapid development and broad application of information and communication technology have greatly enhanced the development and wealth of human society. At the same time, as the world becomes more computerized, the misuse of the products of that computerization presents real threats to the security and stability of individual countries and of the international community as a whole. Such threats include developing and using information weapons, information crime, information terrorism, using leadership in the information field to damage the interests and security of other countries, and disseminating information that undermines the political, economic and social systems and the spiritual cultural environment of other countries. The international community should strengthen its cooperation and jointly respond to these challenges.

2. The Chinese Government has consistently attached a high degree of importance to the issue of information security, and has drafted a series of laws, regulations and standards to protect information security and strictly prohibit all types of criminal network attacks and information systems disruption. In recent years, the Chinese Government has increased its investment in this area and has done a great deal of work on information security, system monitoring and building emergency-response systems; its ability to protect the security of information continues to strengthen as a result.

3. China actively participates in international cooperation in the field of information security. In combating network crime, China's public-security agencies have established close cooperation and investigation-assistance mechanisms with

the police authorities of many countries. China is taking an active role in the work of the international information-security expert group of the Shanghai Cooperation Organization, and working with the other member States of the Organization to find effective ways and means to resolve problems concerning international information security.

4. China holds that the United Nations is the appropriate setting in which to explore the issue of information security, and supports the reconvening by the United Nations in 2009 of a governmental experts group to integrate, on the basis of the work done by the previous governmental experts group in 2004-2005, new developments in information and communications technology and carry out a deep and comprehensive study of the threats and challenges in the field of information security along with effective programmes and policies to address them.

Cuba

[Original: Spanish]
[11 June 2008]

1. Cuba reiterates that the hostile use of telecommunications, with the declared or hidden intent of undermining the legal and political order of States, is a violation of the internationally recognized norms in this area and a negative and irresponsible use of these means, which can give rise to tensions and situations that are not conducive to international peace and security and thereby undermine the principles and purposes enshrined in the Charter of the United Nations.

2. Cuba wishes to underscore the legitimate and prevalent concern of the international community, expressed in General Assembly resolution 62/17 that information and telecommunication technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields.

3. The Government of the United States of America maintains an undeclared war against Cuba that encompasses the information and telecommunications sector, violating the pertinent international norms and laws. It does not consider the damage that it could cause to international peace and security by creating dangerous situations, such as the use of a military aircraft to transmit television signals towards Cuba without its consent. This attitude is inappropriate for a permanent member of the Security Council, which is supposed to assume the fundamental responsibility of maintaining international peace and security on behalf of the other members of the United Nations.

4. The weekly transmissions from United States territory have exceeded 2,300 hours in recent years, using different services and frequency bands. These radioelectric attacks against Cuba violate the principles of international law that govern relations between States and the norms and regulations of the International Telecommunication Union (ITU), which determine the conduct that the member countries of this specialized agency of the United Nations system should follow. At the end of March 2008, a total of 1,889 hours and 15 minutes of illegal weekly transmissions towards Cuban territory from 19 stations using 30 frequencies were recorded.

5. The World Radiocommunications Conference, held in Geneva, Switzerland, from 22 October to 16 November 2007, took a position against the illegal transmissions towards Cuba from an aircraft and indicated that they were not in compliance with the Radio Regulations. Textually, the Conference stated in its conclusions on the case: "a broadcasting station operating on board an aircraft and transmitting solely to the territory of another administration without its agreement cannot be considered in conformity with the Radio Regulations".

6. From the United States territory and with the entire consent of the United States Government, short-wave programmes are transmitted towards Cuba which encourage acts of sabotage, political attacks, the assassination of important people and acts of resistance and deal with other subjects typical of radio terrorism, underscoring the falseness of the declarations by President Bush's Administration regarding its alleged commitment to fighting terrorism.

7. No country has the right to transmit television broadcasts towards another, whether or not such broadcasts adversely affect the other country's services. Cuba has never interfered with the United States television services, let alone used aerostats and aircraft for this purpose.

8. The United States Government's pathological hostility towards Cuba also extends to the Internet. With total cynicism and hypocrisy, it has falsely accused Cuba of preventing its citizens from accessing the global network, while the very different reality is that Cuba is unable to connect to the fibre-optic cables that surround the Cuban archipelago, owing to the embargo laws applied by the United States for nearly 50 years. In addition, without prior notification, the Office of Foreign Assets Control recently blocked .com domains relating to Cuba. This attitude erodes the spirit, the intentions, and the conclusions that prevailed among the nations of the entire world when they met in Switzerland and Tunisia during the World Summit on the Information Society.

9. The World Summit on the Information Society strongly urged States, when building the information society, to take the necessary measures to avoid and refrain from adopting unilateral measures that were not in keeping with international law and the Charter of the United Nations, prevented the full achievement of the economic and social development of the population of the countries affected or adversely affected the well-being of their citizens.

10. The discussion in the General Assembly about developments in the field of information and telecommunications in the context of international security is very pertinent and its timeliness and importance increase every day. Actions such as those described above by the United States of America against Cuba confirm the need for that debate and the urgency of finding solutions that overcome those obstacles to harmony in international relations among States.

11. Cuba strongly supports this exercise by the General Assembly and, consequently, joined the 179 Member States that voted in favour of resolution 62/17, in contrast to the attitude of the United States of America, the only country that voted against it.

12. Cuba will continue to spare no effort in offering its support to the peaceful global development of information and telecommunications technologies and their use for the good of all humanity, and is ready to collaborate with all other countries, including the United States of America, to find solutions that overcome the obstacles that prevent the achievement of these goals.

Jordan

[Original: Arabic]
[16 May 2008]

First: General appraisal of information security issues

Information security is related to the concept of national security and the information security system has a direct connection with telecommunications security, given that it is through wired or wireless networks that information is transmitted. In order to protect and strengthen the security of information and communications the following are required:

- The introduction of regulations, laws and systems to protect the confidentiality, integrity and provision of information and prevent the exploitation of information systems for the commission of crimes;
- The establishment of a strategy for information security, namely, a set of rules that are applied by persons working with the technology and information within the institute. The objectives of the strategy are to familiarize users and administrators with their obligation to protect computer systems and networks as well as to protect data at the stages of input, processing, storage, transfer and retrieval.

Second: Efforts made at the national level

On 20 February 2007 the Government of Jordan established a national technical commission for the security and protection of information, composed of experts from various Government ministries and institutions. The commission's duties have been defined as follows:

- To identify the security, technical, legal and administrative aspects of security and protection of information, information resources and electronic services in Jordan;
- To ensure that the Government's electronic security programmes and projects are in line with security standards in other relevant authorities.

Lebanon

[Original: English]
[29 April 2008]

1. At the national level, the concerned Lebanese authorities, especially the Ministry of the Interior and Municipalities-General Security, are modernizing the information security systems for the internal network and received, in this regard, support from experienced security bodies in friendly countries. However, the necessary and modern equipment is not yet available because of insufficient funding and technological capability.

2. Other concerned Lebanese authorities, mainly the Ministry of the Interior and Municipalities-Internal Security, established a Bureau to Combat Information Crimes and to Protect the Intellectual Property Rights. This Bureau is already functioning.

technologies, which has the support of the African Economic Community. The project led to the preparation of three sets of draft guidelines on electronic commerce, protection of personal data and cybercrime, which will be transmitted shortly to the Conference of Heads of State and Government for adoption.

III. Follow-up at the international level

5. The Office of the High Commissioner for Information and Communication Technologies is either participating in or closely following international projects on the issue.

To this end, the Office of the High Commissioner actively took part in the West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and Critical Information Infrastructure Protection, held in Praia, Cape Verde, from 27 to 29 November 2007. The workshop took place in the context of consultations between the various regions and member countries of the International Telecommunication Union, with a view to implementing the Global Cybersecurity Agenda.

6. In addition, the Office of the High Commissioner also closely followed the work of the Global Forum on Internet Governance and the cybersecurity summit, held in Strasbourg on 1 and 2 April 2008 by the Council of Europe, to strengthen international cooperation between police and legal authorities and Internet service providers.

IV. Activities

7. Lastly, the Office of the High Commissioner for Information and Communication Technologies participates in the work of broadcasting television and radio programmes aimed at raising awareness of the various aspects of cybercrime and information network security in general. It even held a one-day parliamentary briefing on the subject to assist national deputies on 2 May 2008.

8. At the technical level, the Office of the High Commissioner has prepared a draft policy on information security to be implemented by information technology departments and services in government agencies once it has been approved.

9. In conjunction with civil society institutions, the Office of the High Commissioner also periodically organizes information network administration and security training programmes for government personnel and telecommunications operators.

10. A detailed technical note, the terms of reference of the National Information and Communication Infrastructure (NICI) plan focal-point training workshop, the e-Government sectoral strategy, and the draft policy on information system security have been attached for reference.

11. A document on the harmonization of the legal framework for information and communication technologies in West African States (WAEMU-ECOWAS) and the general report on the project on the legal framework for information and communication technologies are available and will be provided to the United Nations as needed.

Qatar

[Original: Arabic]
[7 April 2008]

1. The rapid development and widespread use of information technology (IT) are currently playing a positive part in stimulating economic and social development and improving people's lives around the world. At the same time, data security significantly affects the public security of States and, indeed, the security and stability of the world as a whole. Because all States stand to benefit from it, data security is the shared responsibility of the international community.

2. Qatar believes that the issue of data security involves more than the risks created by the weakness and interwoven nature of information infrastructure. Political, economic, military and social issues are also at stake, not to mention other problems stemming from IT misuse. Each of those issues is relevant to data security analysis.

3. Qatar is convinced that IT should be used in a manner consistent with the Charter of the United Nations and the fundamental principles of international relations. It believes that the free flow of information should be ensured while national sovereignty and security are preserved and historical, cultural and political differences between States are respected. Each State should have the right to manage its own Internet resources in accordance with domestic legislation. In view of the imbalance in technological development between States, Qatar also believes that the international community should support cooperation in respect of IT research and applications, and genuinely affirm IT autonomy for all States.

4. Qatar attaches great importance to IT and is working to implement a national information strategy, having prepared the necessary regulatory legislation. It has made great efforts in support of an Internet security monitoring system. Increasing support is also being provided for basic data protection capacity and crucial information systems.

5. Qatar is convinced that the United Nations constitutes the appropriate forum for consideration of data security issues. It supports the reconvening in 2009 of the Group of Governmental Experts, which will permit an in-depth, comprehensive analysis of the risks and challenges involving data security to be carried out, alongside the formulation of appropriate programmes and policies. As it has done in the past, Qatar will continue to support international efforts to address data security issues.